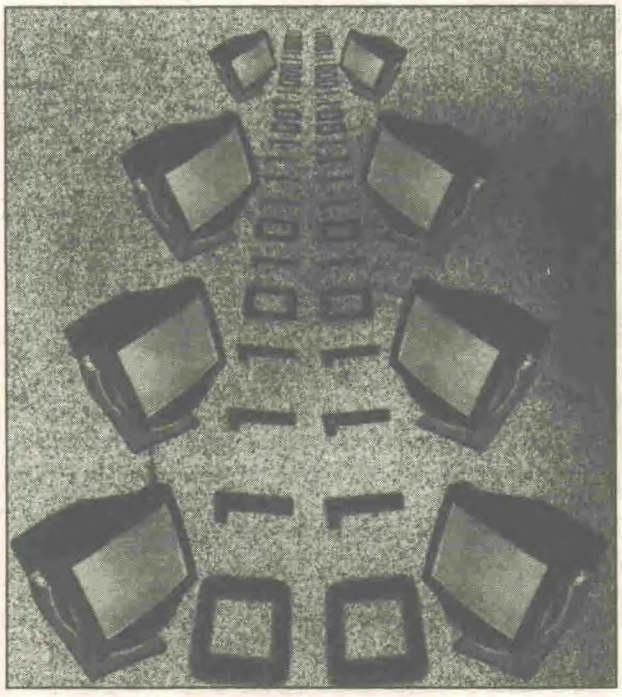
ยืน ภู่วรวรรณ

# กรณีศึกษา : การรักษาความปลอดภัยของระบบคอมพิวเตอร์

*นำเสนอจากประสบการณ์ของผู้เขียน และนำสิ่งที่พบเห็น หรือเคยพบเห็น หรือสิ่งที่ได้มีผู้บอกกล่าว เพื่อให้เป็นตัวอย่าง*



ยุคของเครือข่ายคอมพิวเตอร์ เป็นยุคที่มีการกระจายการใช้งานทรัพยากรคอมพิวเตอร์ไปให้ผู้ใช้ถึงที่ มีการสร้างเส้นทางเชื่อมโยงเครือข่ายคอมพิวเตอร์ การเข้าถึงหรือการใช้งานคอมพิวเตอร์ทำได้ง่ายสะดวกต่อการใช้ ขณะเดียวกันก็สร้างปัญหาในเรื่องการดูแลรักษาความปลอดภัยระบบคอมพิวเตอร์

เพื่อให้เห็นถึงภัยอันตรายจากการโจรกรรมที่บุกรุกเข้ามาในระบบคอมพิวเตอร์ ผู้เขียนจึงขอเสนอบทความ โดยเน้นให้เห็นถึงสภาพที่เกิดขึ้น ซึ่งส่วนหนึ่งเป็นกรณีสมมติ แต่ก็เน้นให้เห็นถึงความเป็นไปได้ และกรณีศึกษาที่เกิดขึ้นนี้เป็นกรณีศึกษาที่อาจมีลักษณะการเกิดขึ้นซ้ำแล้วซ้ำเล่า การศึกษาจากสิ่งเหล่านี้จึงนำเสนอจากประสบการณ์ของผู้เขียน และนำสิ่งที่พบเห็น หรือเคยพบเห็น หรือสิ่งที่ได้มีผู้บอกกล่าว เพื่อให้เป็นตัวอย่าง

## กรณีศึกษาองค์กร ABC

องค์กรที่สมมตินี้มีชื่อองค์กร ABC เป็นองค์กรที่ให้บริการผู้ใช้และพัฒนาระบบสารสนเทศเพื่อให้องค์กรในทุกระดับ โมเดลขององค์กรจึงเป็นส่วนของการพัฒนาระบบซอฟต์แวร์ขึ้นใช้เอง มีเจ้าหน้าที่ทางด้านคอมพิวเตอร์ มีนักวิเคราะห์ระบบ มีผู้ใช้งานในระดับต่าง ๆ และการบริการนี้ยังบริการผู้ใช้ทั้งในองค์กรเอง และบุคคลที่เรียกเข้ามาจากนอกองค์กร

ภายในองค์กรจึงมีระบบคอมพิวเตอร์ของตนเอง และคอมพิวเตอร์เหล่านี้สร้างเป็นเครือข่าย เชื่อมโยงภายในและยังเชื่อมต่อเข้าสู่อินเทอร์เน็ต ผู้ใช้บริการเรียกใช้ได้ทั้งจากภายในบนเครือข่าย จากภายนอกที่เรียกผ่านโมเด็มและผ่านเครือข่ายอินเทอร์เน็ต

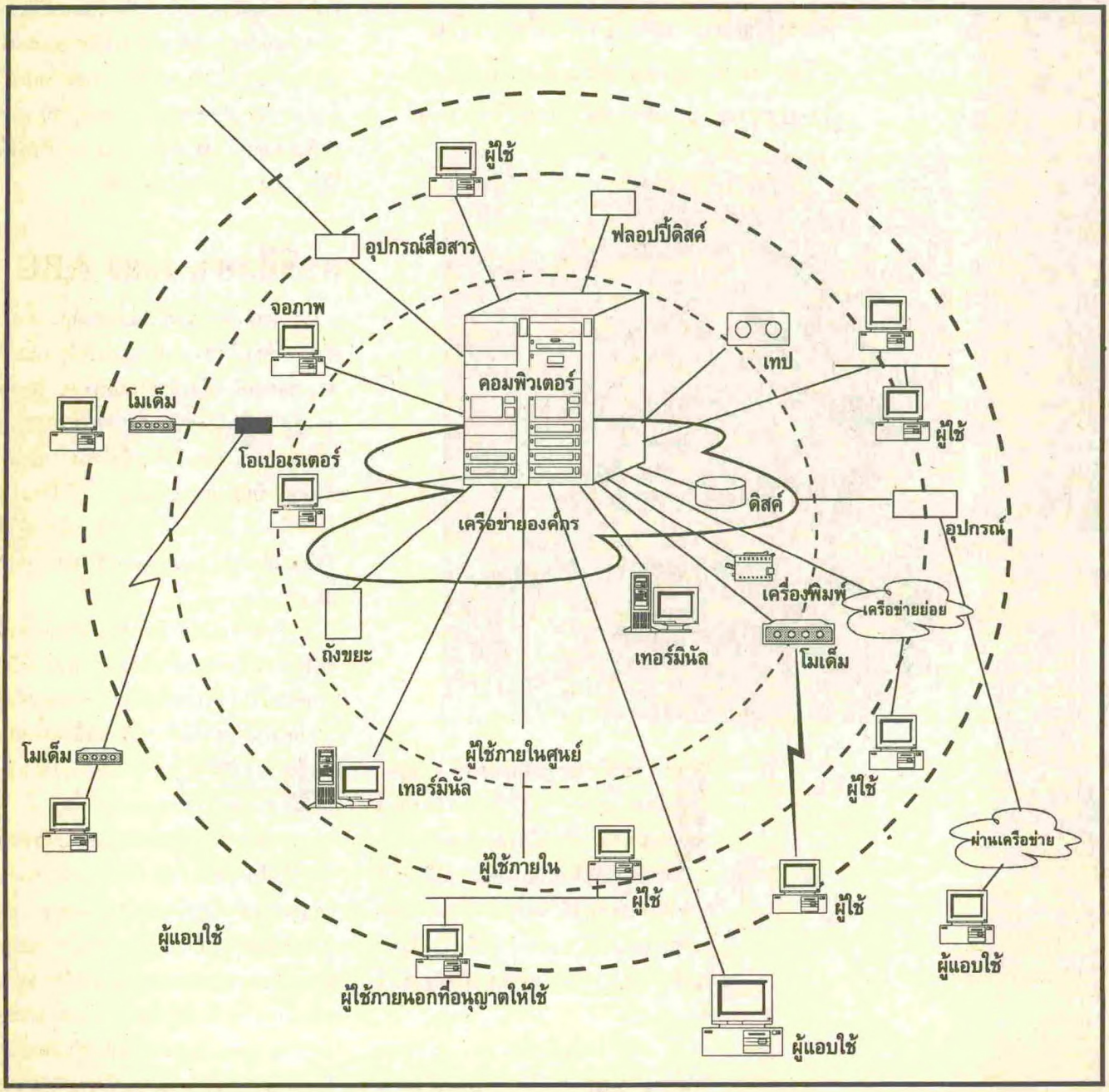
เพื่อสร้างโมเดลระบบคอมพิวเตอร์โดยเน้นในแง่การดูแลและการรักษาความปลอดภัย จึงเขียนรูปโมเดลในลักษณะการวางรูปแบบเพื่อความเข้าใจได้ง่าย การบริหารข้อมูลข่าวสาร การพัฒนาระบบงาน การดำเนินการของทั้งองค์กรจึงมีผู้เกี่ยวข้องในระบบอยู่มากมาย ทุกคนในองค์กรตั้งแต่ผู้บริหารจนถึงพนักงานทั่วไปสามารถเข้าถึงระบบและเรียกใช้ตามฟังก์ชันหน้าที่ของตนเอง

รูปแบบขององค์กรที่สร้างขึ้นเป็นโมเดลตามรูปแบบของระบบการดูแลรักษาความปลอดภัยนี้ เน้นให้เห็นวิธีการเข้าทำลายระบบที่มาจากแหล่งต่าง ๆ และเข้าทำลายระบบในรูปแบบที่แตกต่างกัน การเข้าทำลายนี้มีวิธีการและเทคนิคที่เฉพาะไม่เหมือนกัน

จากรูปแบบที่เสนอได้จัดวงรอบไว้โดยมีระบบอุปกรณ์และฮาร์ดแวร์ภายในอยู่วงกลาง ส่วนของอุปกรณ์เหล่านี้ได้รับการดูแลจากเจ้าหน้าที่ภายในองค์กรเอง รวมถึงผู้พัฒนาระบบงานต่าง ๆ ขององค์กร ตั้งแต่ผู้ป้อนข้อมูล ผู้พัฒนาโปรแกรม ผู้วิเคราะห์ระบบ หรือพนักงานเครื่อง เจ้าหน้าที่เหล่านี้เกี่ยวข้องกับอุปกรณ์ต่าง ๆ ขององค์กรโดยตรง

## การเข้าโจรกรรม

รูปแบบของการเข้าโจรกรรมระบบจึงประกอบด้วยวิธีการหลายอย่าง ซึ่งการเข้าทำลายหรือโจรกรรมระบบประกอบด้วย




รูปที่ 1 โมเดลของระบบรักษาความปลอดภัย

● **การทำลายทางด้านเครื่องมืออุปกรณ์** เป็นการเข้าไปทำในส่วนของตัวระบบสื่อสาร เช่น การแทปสาย การโยกย้ายสาย การเชื่อมต่อ หรือการโยกย้ายอุปกรณ์ เพื่อให้เกิดการทำงานผิดพลาด หรือแม้แต่การลักขโมยอุปกรณ์เครื่องมือต่าง ๆ

● **การทำลายข้อมูล** เป็นการเข้าไปถึงตัวข้อมูล ทำลายข้อมูล หรือจัดการแก้ไขข้อมูลให้ผิดพลาด ทำให้โปรแกรมทำงานผิดพลาด วางโปรแกรมเข้าไปทำลาย เช่น การใส่ไวรัส ใส่ Trojan เป็นต้น

● **การโกงหรือเปลี่ยนแปลงข้อมูล** เป็นวิธีการที่เข้าไปถึงข้อมูล แก้ไขข้อมูลบางส่วนเพื่อประโยชน์ของตนเองหรือของกลุ่ม เข้าไปแก้ไขโปรแกรมเพื่อให้ทำงานกับข้อมูลผิดพลาด

● **แอบใช้บริการ** เป็นวิธีการเรียกเข้าระบบเพื่อใช้บริการต่าง ๆ โดยไม่มีสิทธิ์ในการใช้ แอบเข้าไปในระบบเพื่อรันโปรแกรมเพื่อใช้งานบางอย่าง เช่น ผู้ใช้อินเทอร์เน็ตแอบเข้าไปเพื่อเป็นทางผ่านไปยังระบบอื่น

● **แอบดูข้อมูล** เป็นการเรียกเข้าระบบเพื่อแอบดูข้อมูลความลับบางอย่าง ค้นหาข้อมูลในส่วนที่เป็นความลับ

● **ขโมยข่าวสาร** เป็นการนำเอาข่าวสารที่ไม่ต้องการเปิดเผย หรือแอบนำข่าวสารบางอย่างไปใช้ประโยชน์เพื่อตนเองหรือหมู่คณะ

จากโมเดลที่เขียนไว้ในรูปที่ 1 จะเห็นว่าปัญหาของโจรกรรมที่เกิดขึ้นในระบบจะเกี่ยวข้องกับบุคคลต่าง ๆ โดยอาจมีบุคคลภายในให้ความร่วมมือหรือเป็นผู้ดำเนินการเอง หากนำมาเขียนเป็นรูปภาพความสัมพันธ์ของบุคคลกับการที่จะมีส่วนเกี่ยวข้องในการโจรกรรม เขียนได้ดังรูปที่ 2

## กรณีศึกษาที่ 1 การทำให้เกิดการเสียหายกับเครื่องมืออุปกรณ์

พนักงานภายในห้องทำงานได้นำดิสเกตต์ไปใช้ส่วนตัว โดยนำแผ่นดิสเกตต์ที่เจ้าหน้าที่พัฒนาระบบงานได้วางไว้ ผลคือ งานที่เจ้าหน้าที่พัฒนาระบบงานนั้นมีโปรแกรมที่กำลังเขียนค้างไว้ ผลที่เกิดขึ้นคือต้องเสียเวลาในการเขียนใหม่หรือทำงานใหม่ ซึ่งต้องใช้เวลาไม่น้อยกว่าหนึ่งสัปดาห์

การทำให้เกิดความเสียหายกับเครื่องมืออุปกรณ์ ในกรณีของผู้ที่มีความรู้จะเป็นเรื่องที่จับได้ยาก เช่น พนักงานควบคุมเครื่องได้แอบดำเนินการย้ายสายเชื่อมโยงระบบสื่อสาร เพื่อให้เพื่อนของตนเองสามารถเรียกเข้าสู่ระบบได้ โดยไม่ต้องผ่านอุปกรณ์ไฟร์วอลล์ (firewall) หรืออุปกรณ์ตรวจจับทำให้สามารถเข้าสู่ระบบได้โดยไม่มีการเก็บประวัติหรือสกรีนการใช้งาน

## กรณีศึกษาที่ 2 แอบใช้บริการ

พนักงานเขียนโปรแกรมของบริษัทได้รับงานภายนอกบริษัทเข้ามาทำเป็นงานส่วนตัว รับจ้างเขียนโปรแกรมเฉพาะที่ต้องใช้ซอฟต์แวร์สำเร็จ การกระทำดังกล่าวได้กระทำโดยการใช้ทรัพยากรทั้งหมดขององค์กร โดยการเก็บข้อมูล เก็บโปรแกรม และทำการรันคอมพิวเตอร์เพื่อให้ได้ผลลัพธ์ แล้วนำผลลัพธ์นั้นไปใช้ประโยชน์เพื่อผลประโยชน์ของตนเอง การดำเนินการในลักษณะนี้มีลักษณะเป็นการแอบใช้งาน ในเวลาต่อมาผู้จัดการแผนกจับได้ จึงได้ลงโทษภาคทัณฑ์ไว้

## กรณีศึกษาที่ 3 ทำลายข้อมูล

กลุ่มแฮกเกอร์สามคน ใช้เครือข่ายสาธารณะอินเทอร์เน็ตเข้าสู่ระบบคอมพิวเตอร์ของบริษัท กลุ่มนี้ได้เข้าสู่ระบบโดยใช้ความ

**รูปที่ 2 ความสัมพันธ์ของบุคคลกับการกระทำผิดที่มักพบบ่อย**

| | โอเปอเรเตอร์ | โปรแกรมเมอร์ | พนักงานป้อนข้อมูล | ผู้ใช้ภายในองค์กร | ผู้ใช้ภายนอกองค์กร | แฮกเกอร์ผู้บุกรุก |
|---|---|---|---|---|---|---|
| ทำลายเครื่องมืออุปกรณ์ | X | | | | | |
| ทำลายข้อมูล | X | X | | | X | X |
| โกงหรือเปลี่ยนแปลงข้อมูล | | X | X | | | X |
| แอบใช้บริการ | | X | | X | X | X |
| แอบดูข้อมูล | | | | X | X | X |
| ขโมยข่าวสาร | X | | | X | X | X |

รู้จักกับคนภายในขอยืม account name เพื่อใช้ชั่วคราว แต่เมื่อเข้าสู่ระบบได้ มีการคัดลอกแฟ้ม password ของระบบไปทั้งหมด หลังจากนั้นนำข้อมูลแฟ้ม password ไปทำการถอดรหัสด้วยโปรแกรม crack ที่มีแพร่หลายอยู่บนอินเทอร์เน็ต ผลปรากฏว่าสามารถถอดรหัสผ่านของบุคคลในแฟ้ม password ได้เป็นจำนวนมาก

กลุ่มแฮกเกอร์นี้ได้ดำเนินการต่อโดยการเข้าสู่ระบบจากรหัสที่ถอดได้ผ่านทางอินเทอร์เน็ต หลังจากนั้นเข้าไปรื้อค้นระบบไฟล์ต่าง ๆ รวมทั้งสามารถเบรกระบบเพื่อแก้ไขไฟล์ระบบบางส่วนได้ และวางโปรแกรมประเภท Trojan ไว้ นอกจากนี้ยังมีการลบไฟล์ที่เป็นประวัติการใช้งานบางส่วนออกไป

การดำเนินการของกลุ่มแฮกเกอร์นี้ได้ดำเนินการกว่า 3 เดือน ผู้ดูแลระบบเกิดสงสัยจึงได้วางกับดักไว้ และด้วยความร่วมมือที่ดีขององค์กรอื่นที่แฮกเกอร์เรียกผ่าน ทำให้สามารถจับแฮกเกอร์ทั้งสามคนได้

## กรณีศึกษาที่ 4
## แอบใช้บริการ

บริษัทให้บริการอินเทอร์เน็ตส่วนใหญ่มีโมเด็มไว้ให้บริการ การใช้บริการจะเป็นการบริการเฉพาะตัว ปรากฏว่ามีผู้ใช้บริการส่วนหนึ่งนำรหัสผ่านของตัวเองแจกผู้อื่นให้ใช้ร่วม การดำเนินการในลักษณะนี้ยากที่จะตรวจสอบได้ว่าใครคือผู้ใช้ตัวจริง หรือใครคือผู้ใช้ตัวปลอม

บริษัทให้บริการอินเทอร์เน็ต จึงเขียนโปรแกรมตรวจสอบการเรียกเข้าสู่ระบบ หากมีการเรียกเข้าสู่ระบบจากโมเด็มพร้อมกันสองสาย หรือเรียกจากโมเด็มหนึ่งสาย โดยขณะเรียกเข้ามามีผู้ใช้ตามบัญชีชื่อนี้ใช้อยู่ก่อน ระบบจะตรวจสอบว่ามีการนำชื่อบัญชีไปให้ผู้อื่นใช้ ระบบจะปิดบัญชีผู้ใช้นั้น

## กรณีศึกษาที่ 5
## การวาง Trojan houses

โทรจัน คือเรื่องนิยายปรัมปราที่กล่าวถึงสงครามเมืองทอย เมืองทอยแข็งแรงมาก ข้าศึกไม่สามารถที่จะตีได้ ต่อมาวันหนึ่งข้าศึกได้สร้างม้าไม้ไว้หนึ่งตัวแล้วนำมาวางไว้หน้าประตูเมือง เพื่อล่อ ปรากฏว่าทหารเมืองทอยเห็นม้าไม้ก็สนใจลากม้าไม้เข้าเมือง ตกกลางคืนทหารที่ซ่อนในห้องม้าไม้ออกมาเปิดประตูเมือง ทำให้ข้าศึกเข้าเมืองทอยและสามารถตีเมืองทอยแตกได้

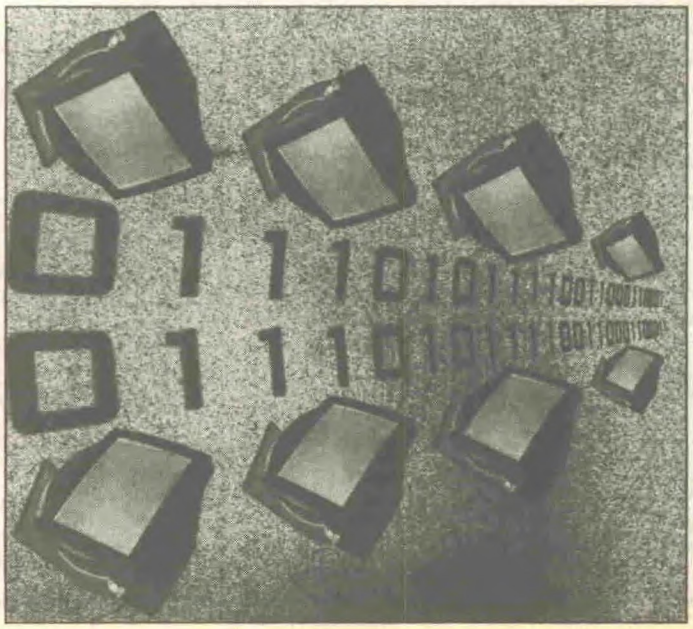
โปรแกรมที่นำมาแอบวางไว้ในระบบจึงถือว่าเป็นโทรจัน ซึ่งจะพบเห็นได้มากในระบบรักษาความปลอดภัย

- **การสร้างเชลหลอก** แฮกเกอร์จำนวนมากชอบสร้างโปรแกรมประเภทโทรจันไว้หลอก เช่นสร้างเชลโปรแกรมใหม่ไว้หลอก โดยโปรแกรมเชลใหม่นี้จะมีหน้าตาเหมือนโปรแกรมเชลเดิม ผู้ใช้จะไม่รู้ และโปรแกรมเชลนี้จะเก็บข้อมูลต่าง ๆ ที่ผู้ใช้กดแป้นพิมพ์เอาไว้ ทำให้รู้ว่าผู้ใช้กดแป้นพิมพ์อะไรบ้าง จึงสามารถล่วงรู้รหัสผ่านที่เรียกไปยังเครื่องอื่นหรือระบบอื่นได้

- **การสร้าง .rlogin ไว้** ในกรณีที่แฮกเกอร์เข้าระบบได้โดยผ่านทางยูสเซอร์ใดและยูสเซอร์นั้นไหวตัวอาจเปลี่ยนรหัสผ่านไป วิธีการที่ทำให้ไม่ขึ้นกับรหัสผ่านคือการใส่ข้อมูลไว้ใน .rlogin เพื่อว่าครั้งต่อมาเรียกเข้าสู่ระบบโดยตรงโดยไม่ต้องใช้รหัสผ่าน ลักษณะของการใส่ข้อมูลในแฟ้ม .rlogin ก็เป็นวิธีหนึ่งของแฮกเกอร์ที่ชอบใช้

- **การเขียนไฟล์ระบบเพื่อเปิดให้เรียกเข้าได้ในภายหลัง** ผู้ดูแลระบบที่ไม่จัดเจนโดยเฉพาะผู้ดูแล root หากมีผู้เบรกเข้าสู่ root ได้ อาจสร้างเชลหลอกหรือสร้างเงื่อนไขของโปรแกรมระบบบางที่ไว้ เพื่อทำให้ผู้เข้ามาภายหลังสามารถเข้าสู่ระบบในลักษณะที่ไม่ต้องใช้รหัสผ่านอีกต่อไป การสร้างโปรแกรมหรือการดำเนินการในลักษณะนี้กระทำได้หลายวิธีการ

- **การเปลี่ยนโปรแกรมที่มีช่อง** แฮกเกอร์ที่ชำนาญและมีความรู้อาจเข้าสู่ระบบได้ครั้งหนึ่งด้วยวิธีการใดก็ตาม เมื่อเข้าได้แล้วก็จะเปิดช่องไว้เพื่อเรียกเข้าครั้งต่อไปได้ง่าย หรือแม้แต่ผู้ดูแลระบบไหวตัวก็สามารถเข้าได้ง่ายในภายหลัง ในกรณีนี้มีวิธีการทำโดยการนำโปรแกรมบางโปรแกรมที่มีการดัดแปลงให้มีช่องโหว่ไว้มาเปลี่ยนแปลงหรือแทนโปรแกรมเดิม เช่นนำโปรแกรมเอดิเตอร์ตัวใหม่มาใส่ไว้ โปรแกรมที่ใส่นี้มีช่องโหว่ที่เข้าสู่ระบบได้



การวางโทรจันมีวิธีการที่ทำได้หลายอย่าง บางครั้งทำการแก้ไขโปรแกรมที่ผู้เรียกใช้เพื่อทำให้โปรแกรมดังกล่าวเก็บข้อมูลบางส่วนไว้ หรือสร้างช่องเพื่อการทำงานบางอย่าง

อย่างไรก็ดี ปัจจุบันมีโปรแกรมที่ใช้ในการสแกนดูแฟ้มทั้งหมด โดยดูว่าแฟ้มใดเป็นที่น่าสงสัยหรือมีการแก้ไข หรือมีการวางเพิ่มเติมเข้ามาในระบบ โปรแกรมสแกนเหล่านี้ทำให้สามารถตรวจจับโทรจันได้

## กรณีศึกษาที่ 6 การแทปสาย

นักศึกษาทางวิชาวิศวกรรมคอมพิวเตอร์ในญี่ปุ่นสองคน ได้ใช้ออสซิลไลสโคปและเครื่องบันทึกสัญญาณ ซึ่งเป็นเพียงแค่เครื่องบันทึกเสียงธรรมดา บันทึกสัญญาณจากสายเอทีเอ็มที่ติดต่อกับธนาคารพาณิชย์แห่งหนึ่ง ทำให้เขาได้รหัสของบัตรเอทีเอ็มของลูกค้าสามราย เขาสามารถใช้รหัสถอนเงินได้กว่า 2 ล้านเยนในเวลาเพียง 3 ชั่วโมง แต่ในที่สุดนักศึกษาทั้งสองคนนี้ก็โดนจับได้และได้รับข้อหาอาชญากรรมไปในที่สุด

## กรณีศึกษาที่ 7 ประตูหลัง

ในการพัฒนาโปรแกรมคอมพิวเตอร์ ผู้พัฒนาโปรแกรมระบบฐานข้อมูลหรืองานที่เกี่ยวข้องกับข้อมูลมักจะเขียนโปรแกรมเฉพาะไว้สำหรับตนเอง เพื่อจะได้เรียกเข้าไปแก้ไขหรือตรวจสอบข้อมูลได้ โดยไม่เกี่ยวข้องกับการทำงานตามปกติของโปรแกรม โปรแกรมประเภทนี้บางทีก็เรียกว่า backdoor หรือประตูหลัง เพื่อที่จะมีช่องทางเข้าสู่ข้อมูลได้

บางครั้งผู้พัฒนาลืมยกเลิกโปรแกรมนี้หรือไม่นำโปรแกรมนี้ออกจากระบบ ทำให้แฮกเกอร์ค้นพบได้โดยบังเอิญ การค้นพบนี้ทำให้สามารถเข้าสู่ระบบและแก้ไขข้อมูลได้ ดังเช่นภาพยนตร์เรื่องวอร์เกม ที่เด็กนักเรียนสามารถเข้าสู่ประตูหลังแล้วไปแก้ไขเกรดของตนเองจนได้ A หมดทุกวิชา หรือในภาพยนตร์เรื่อง The Nets บริษัทผู้พัฒนาซอฟต์แวร์แอบทำประตูหลังเอาไว้ ดังนั้นเขาสามารถเข้าถึงข้อมูลของรัฐบาลได้ทั้งหมด การวางประตูหลังไว้จึงเป็นเรื่องที่น่ากลัวสำหรับผู้ซื้อซอฟต์แวร์ ซึ่งเมื่อเร็ว ๆ นี้ก็มีข่าวว่าบริษัทผู้ผลิตซอฟต์แวร์รายใหญ่หนึ่งแอบใส่โปรแกรมเพื่อเก็บข้อมูลของลูกค้าส่งมาทางเครือข่ายให้กับตนเอง

## การตรวจสอบกลโกง

เรื่องนี้เป็นเรื่องที่ต้องคิดไว้ตั้งแต่เริ่มต้น การตรวจสอบกลโกงต่าง ๆ จำเป็นจะต้องมีและกระทำไว้อย่างดี วิธีการตรวจสอบกลโกงหรือตรวจสอบแฮกเกอร์ต้องกระทำและร่วมมือกันในระดับผู้ดูแลระบบบนเครือข่าย โดยเฉพาะเครือข่ายอินเทอร์เน็ต

เทคนิคที่ใช้ในการตรวจสอบกลโกงต่าง ๆ เหล่านี้กระทำได้หลายอย่าง เช่น

- **การเก็บประวัติ wtmp** เป็นการเก็บ lastlog หรือประวัติการเรียกเข้าสู่ระบบว่ามีใครเข้าสู่ระบบบ้าง เข้ามาเมื่อไร เลิกใช้เมื่อใด และมาจากที่ใด อย่างไรก็ตาม แฟ้มนี้สามารถแก้ไขเปลี่ยนแปลงได้ ดังนั้นผู้ดูแลระบบอาจต้องหาวิธีการป้องกันแฟ้มนี้ไว้ โดยการเก็บไว้ในที่ที่ผู้อื่นไม่สามารถเปิดดูได้ หรือมีการส่งข้อมูลไปเก็บไว้ที่อื่น เป็นการสำเนาอีกครั้งทุกขณะที่มีการเขียนแฟ้ม
- **การเก็บโปรเซสของการใช้** นอกจากเก็บประวัติการใช้แล้วอาจต้องเก็บประวัติของโปรเซสว่าผู้ใช้แต่ละคนเรียกโปรแกรมใดมาใช้บ้าง เพื่อการตรวจสอบ
- **การตรวจสอบข้อมูล** แฟ้มข้อมูลที่เก็บและเป็นแฟ้มสำคัญจะมีวิธีการในการบอกได้ว่าแฟ้มดังกล่าวมีการแอบแก้ไขหรือไม่ เช่น มีการใส่รหัส checksum ไว้ที่อื่น ดังนั้นหากมีการแก้ไขโดยไม่ถูกต้อง ค่า checksum จะผิดไป
- **การวางโปรแกรมตรวจสอบบางชนิด เช่น indent deamon** โปรแกรมนี้จะเป็นการให้ข้อมูลว่าการเรียกเข้าระบบในเครือข่ายมาจากเครื่องใด และยูสเซอร์ชื่อใด การเรียกใช้นี้จะมีการโยงได้ว่าเป็นใคร มาจากไหน ข้อมูลเหล่านี้จะได้รับการเก็บไว้หมด

หลายบริษัทจึงออกกฎห้ามพนักงานใช้โมเด็มเชื่อมต่อเข้ากับระบบเครือข่ายขององค์กร เพราะโมเด็มผ่านทางเครือข่ายโทรศัพท์ทำให้ไม่สามารถตรวจสอบได้ว่าต้นทางเป็นผู้ใด แต่หากเรียกจากเครือข่ายด้วยกันเองจะทำให้สามารถ trace ไปได้ว่าเป็นผู้ใดใช้

- **การหมั่นดูแลของผู้ดูแลระบบ** ผู้ดูแลระบบจะเป็นผู้ที่คุ้นเคยกับพฤติกรรมการใช้งานของบุคคลในระบบ ดังนั้นหากมีข้อผิดปกติหรือข้อสงสัย ผู้ดูแลระบบสามารถตรวจสอบได้ง่ายและรวดเร็ว ดังนั้นผู้ดูแลระบบจะเป็นผู้ที่มีความสำคัญที่จะป้องกันปัญหาที่อาจเกิดความเสียหายต่อระบบได้

## จริยธรรมและการลงโทษขั้นรุนแรง

อาชญากรรมทางคอมพิวเตอร์นับวันจะรุนแรงมากยิ่งขึ้น สิ่งที่สำคัญจึงอยู่ที่การสร้างจิตสำนึกและจริยธรรมของผู้ใช้ หรือผู้เกี่ยวข้องระบบทั้งหมด เพราะหากผู้ที่มีความรู้และมีจิตใจเป็นโจรแล้ว จะเป็นโจรที่มีความรู้และน่ากลัวยิ่งกว่าโจรที่เป็นข่าวในหน้าหนังสือพิมพ์

ดังนั้นทุกองค์กรและหน่วยงานจะต้องเน้นว่าอาชญากรรมทางด้านคอมพิวเตอร์เป็นเรื่องที่รุนแรง หากตรวจพบได้จะต้องลงโทษขั้นรุนแรง การสร้างจิตสำนึกจึงเป็นเรื่องที่จะลดปัญหาในอนาคตได้ อย่างน้อยก็ลดความรุนแรงของอาชญากรรมลงได้บ้าง